CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

July 26, 2022

Bots for Stealing One-Time Passwords Simplify Fraud Schemes

This report details how one-time password (OTP) bypass bots work, how they fit into existing fraud schemes, and the threats they pose to individuals and financial institutions. The report also includes a tutorial on how cybercriminals configure and use OTP bypass bots. The sources for this report include dark web forums, fraud-focused Telegram channels, and the Recorded Future Payment Fraud Intelligence module. The report is intended for fraud and cyber threat intelligence (CTI) teams at financial institutions and security researchers.

Executive Summary

A one-time password (OTP) is a form of multi-factor authentication (MFA) that is often used to provide an additional layer of protection beyond basic passwords. OTPs are dynamic passwords that typically consist of 4 to 8 numbers but may also occasionally include letters. Many financial institutions and online services use this tool to authenticate logins, confirm transactions, or identify users. The main way to provide an OTP code to a user is via SMS, email, or a mobile authentication application such as Authy. Since OTPs protect victims' accounts from unauthorized access or transactions, cybercriminals are constantly developing various ways to bypass and overcome them.

Over the past year, threat actors have increasingly developed, advertised, and used bots to automate the theft of OTPs, making it easier and cheaper for threat actors to bypass OTP protections at scale. Because OTP bypass bots require little technical expertise and minimal language skills to operate, OTP bypass bots also increase the number of threat actors capable of bypassing OTP protections. OTP bypass bots typically function by distributing voice calls or SMS messages to targets, requesting the targets to input an OTP, and, if successful, sending the inputted OTP back to the threat actor operating the bot.

Recorded Future analysts identified and tested an open-source OTP bypass bot named "SMSBypassBot" that was advertised on a fraud-focused Telegram channel and confirmed that it worked as advertised and was simple to configure and use.

Key Findings

The increased use of OTPs by a variety of legitimate services (particularly for authenticating online account logins, money transfers, and 3-Domain Secure-enabled [3DS] purchases) creates parallel cybercriminal demand for methods of obtaining and bypassing OTPs.

Dark web forum activity related to OTP bypassing (measured by volume of posts and views of posts related to the topic) rose sharply in 2020 and has remained high since.

Traditional methods of OTP bypassing (performing SIM card swaps, brute-forcing, abusing poorly configured authentication systems, and manual social engineering) have become time-consuming and more technically challenging.

OTP bypass bots combine social engineering and voice phishing (vishing) techniques with simple-to-use interfaces to provide a partially automated, affordable, and scalable method of obtaining victims' OTPs.

Background

Multi-factor authentication (MFA) provides an additional layer of security beyond just a static password, with Microsoft reporting that MFA can block over 99.9% of account compromise attacks. One-time passwords (OTPs) are a form of MFA that use an automatically generated string of characters (typically numeric values but occasionally alphanumeric) to authenticate a user.

Service providers, financial institutions, and merchants use OTPs for a variety of purposes including authenticating online account logins, money transfers, and 3DS-enabled payment card transactions. Increased adoption of OTPs over the past decade has caused threat actors to develop methods of bypassing OTPs to gain unauthorized access to online accounts and conduct fraudulent money transfers and transactions.

Threat Analysis

The Danger of OTP Bypass

MFA, and more specifically the use of OTPs, means that if threat actors obtain a victim's login credentials for a given service, there is still another layer of security protecting the account. Implementation of OTPs has increased the demand for new fraud techniques in order for cybercriminals to access compromised accounts. OTP-bypassing techniques and bots serve a wide range of use cases for threat actors, encompassing bank, wire, and card fraud as well as other schemes that require access to a specific account within a larger set of steps. As shown in the table below, cybercriminal interest in OTP bypassing rose sharply in 2020 and has remained high since.

In the context of bank fraud, bypassing an OTP can be used to authorize online bank account logins and confirm money transfers, such as via Zelle, or authorize bank accounts to be linked to payment services such as Google Pay or Apple Pay.

In the context of card fraud, 3DS protocol incorporates OTPs as one method of several for authenticating transactions. This means that 3DS-enabled merchants who incorporate OTPs into their authentication flow would require threat actors to obtain the OTP to monetize compromised payment cards, even if they have the relevant payment card data and billing information. Due to higher 3DS adoption rates in Europe, OTPs are more frequently required for transactions involving a European-issued card and a European merchant than in parallel transactions in North America, thereby corresponding to higher cybercriminal demand for OTP-bypassing tools in the card fraud space.

Development of a New Method for OTP Bypass

Historically, cybercriminals have relied on 4 primary methods of bypassing OTP requirements to obtain victims' OTPs: performing SIM card swaps, brute-forcing, abusing poorly configured authentication systems, and manual social engineering. However, as shown in the table below, each of these methods has become less attractive due to technical impediments or excessive time requirements.

Method	Description	Drawback
SIM Card Swap	Obtain access to a target's SIM card and directly receive OTP.	It is prohibitively time-consuming and expensive to perform SIM card swaps at scale.
Brute force	Use a tool to attempt OTP combinations until access is granted.	Modern login systems almost always enforce a passcode submission limit.
Abuse authentication system	Identify services in which the confirmation function accepts any random value.	It is extremely rare for modern authentication systems to accept any random value.
Manual social engineering	Call or message the target while pretending to be a legitimate entity and ask for the OTP.	It is prohibitively time-consuming to perform at scale and requires near-native-level language skills.

Table 1: Historically predominant ways to obtain OTPs from victims (Source: Recorded Future)

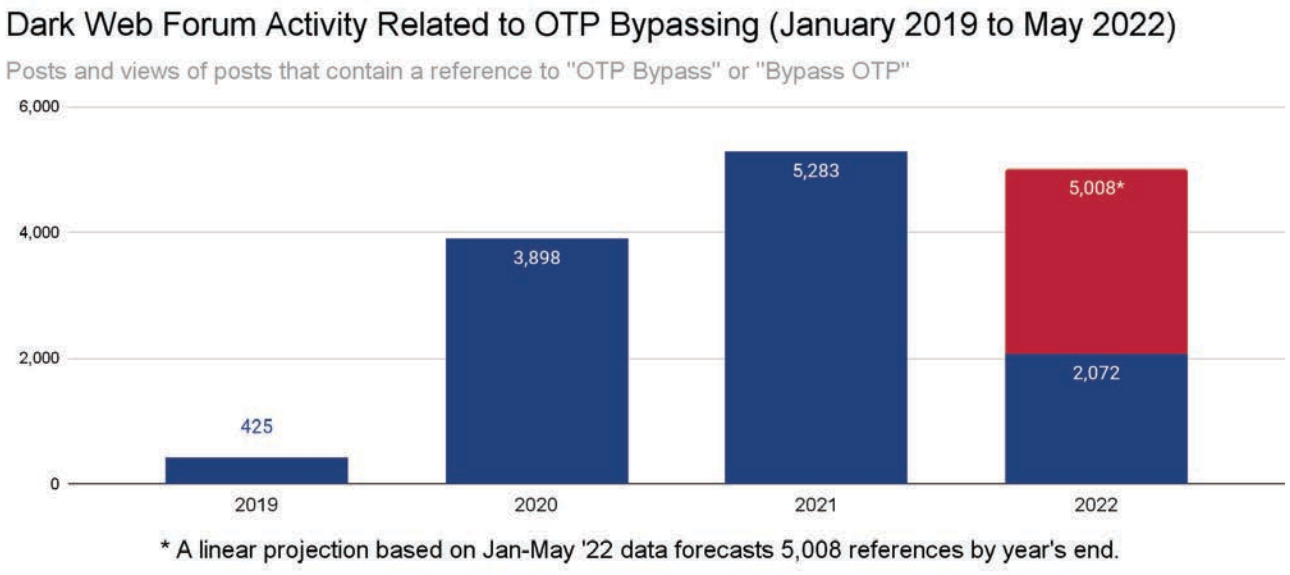


Figure 1: Dark web forum activity related to OTP bypassing rose sharply in 2020 and has remained high since (Source: Recorded Future Payment Fraud Intelligence module)

As the first 3 methods listed in the table above are no longer viable methods for bypassing OTPs, cybercriminals now overwhelmingly rely on social engineering. However, even disregarding the time-consuming nature of social engineering at scale, performing social engineering requires strong language and persuasion skills to succeed at a profitable rate. Despite this, cybercriminal groups do establish "call centers" and recruit specialists with linguistic and social engineering skills. Problems with this scheme include staff turnover and the risk that a new hire might be a law enforcement informant.

In response to high cybercriminal demand for viable and cost-effective methods for bypassing OTPs, threat actors have developed "OTP bypass bots" over the past year. These OTP bypass bots automate time-tested social engineering techniques to provide higher success rates at a fraction of the cost of criminal call centers. More broadly, the advent of OTP bypass bots fits in the current trends toward "software-as-a-service" (SaaS) in the cybercriminal sphere. In the same way that Magecart-as-a-service and phishing-as-a-service (PhaaS) have dramatically reduced the technical expertise and time required to engage in these criminal endeavors, OTP bypass bots lower the entry barrier for gaining access to OTP-protected accounts.

OTP Bypass Bots

OTP bypass bots operate through a simple method: the threat actor provides a target's phone number and the bot then initiates a phone call (or SMS message) that recites a preconfigured recording designed to deceive the target into providing the OTP issued by a legitimate service. When performing this type of vishing attack, the threat actor will align the phone call with a login attempt that prompts the given entity to send out an OTP passcode. If the target falls for the vishing attempt, the target types the OTP passcode into their phone keypad after being prompted by the recording. The threat actor would then receive the OTP, gain access to the account, and proceed with their scheme.

Over the past year, threat actors have advertised various OTP bypass bots on dark web forums and fraud-focused Telegram channels. In keeping with other criminal services, the OTP bypass bots are offered on a rental basis with typical prices averaging several hundred dollars per month. As shown in the example below, the operators of the OTP bypass bot "GRABotpbot" claim it can be used to obtain OTPs for services like Apple Pay, PayPal, and Zelle, as well as obtaining codes for 3DS-protected transactions, wire transfers, and unspecified "online accounts".

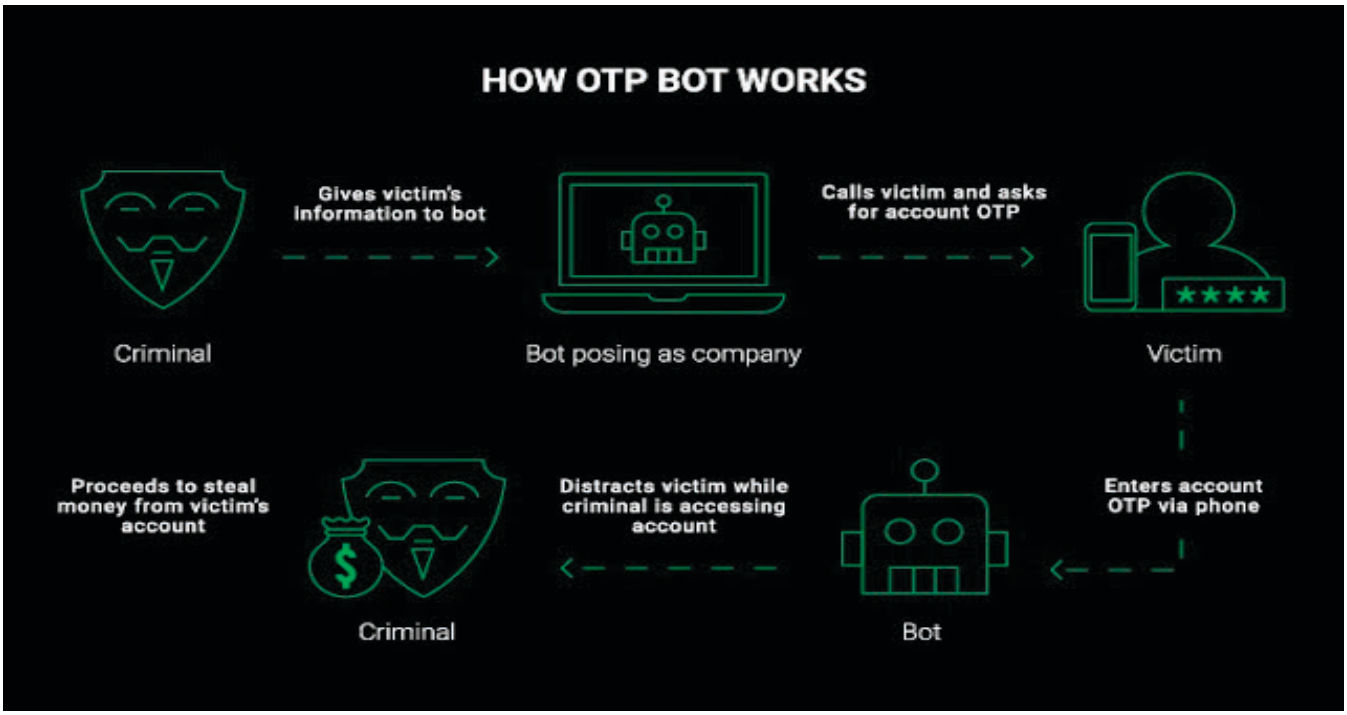


Figure 2: A workflow created by the creator of the OTP bypass bot SMSBypassBot showing how OTP bypass bots fit into fraud schemes (Source: SMSBypassBot page on GitHub)

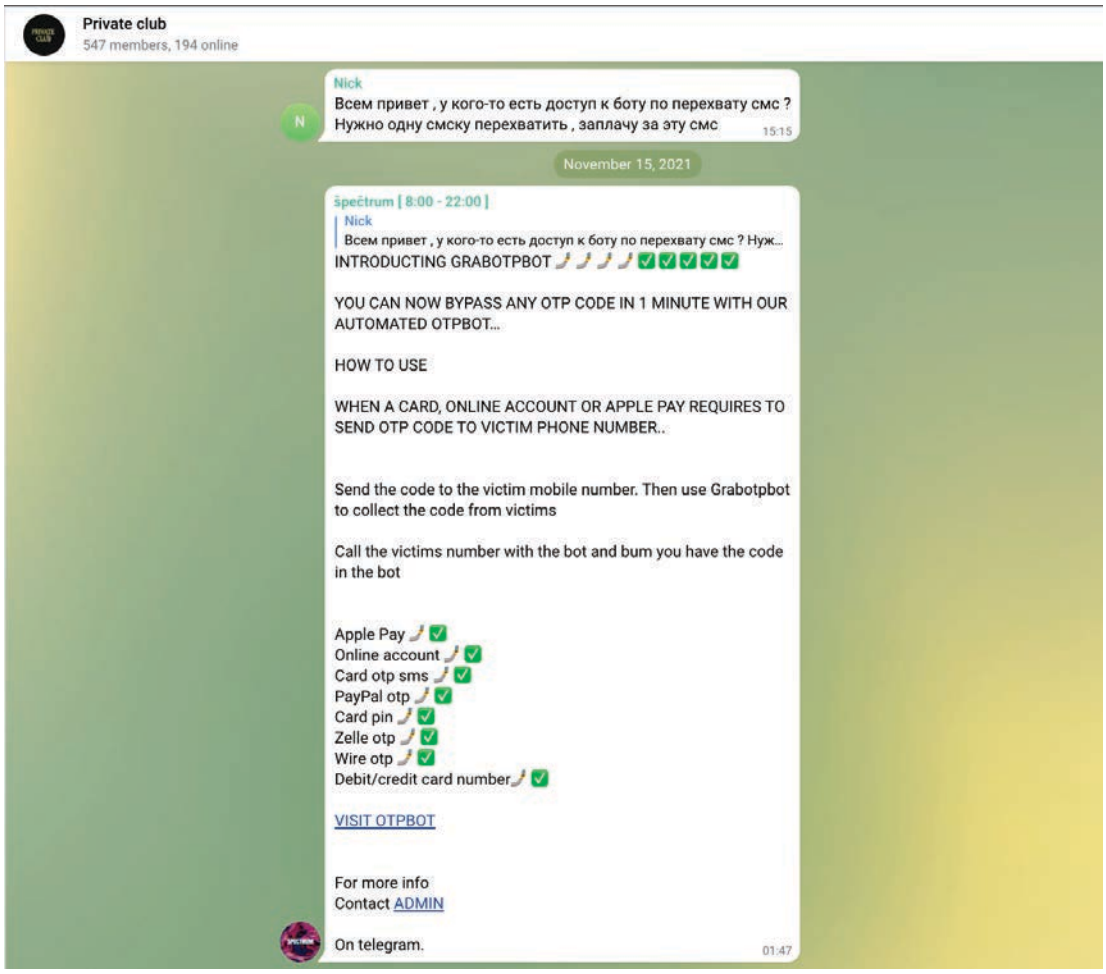


Figure 3: The actor "špečtrum [8:00 - 22:00]" advertises the OTP bypass bot "GRABotpbot" in the Telegram channel "Private club" (Source: Telegram)

Threat actors are typically wary of using proprietary criminal services like GRABotpbot out of fear that the operators may have designed the service to intercept data compromised by criminal users of the service. As a result, criminal services that are open-source generally attract higher confidence from threat actors. One prominent example of an open-source OTP bypass bot is SMSBotBypass, which was posted to GitHub on December 26, 2020 by the user "Ross1337". The GitHub page for SMSBotBypass was deleted in mid-February 2022; however, the bot was advertised on Telegram channels and several copies of the source code were produced prior to the deletion.

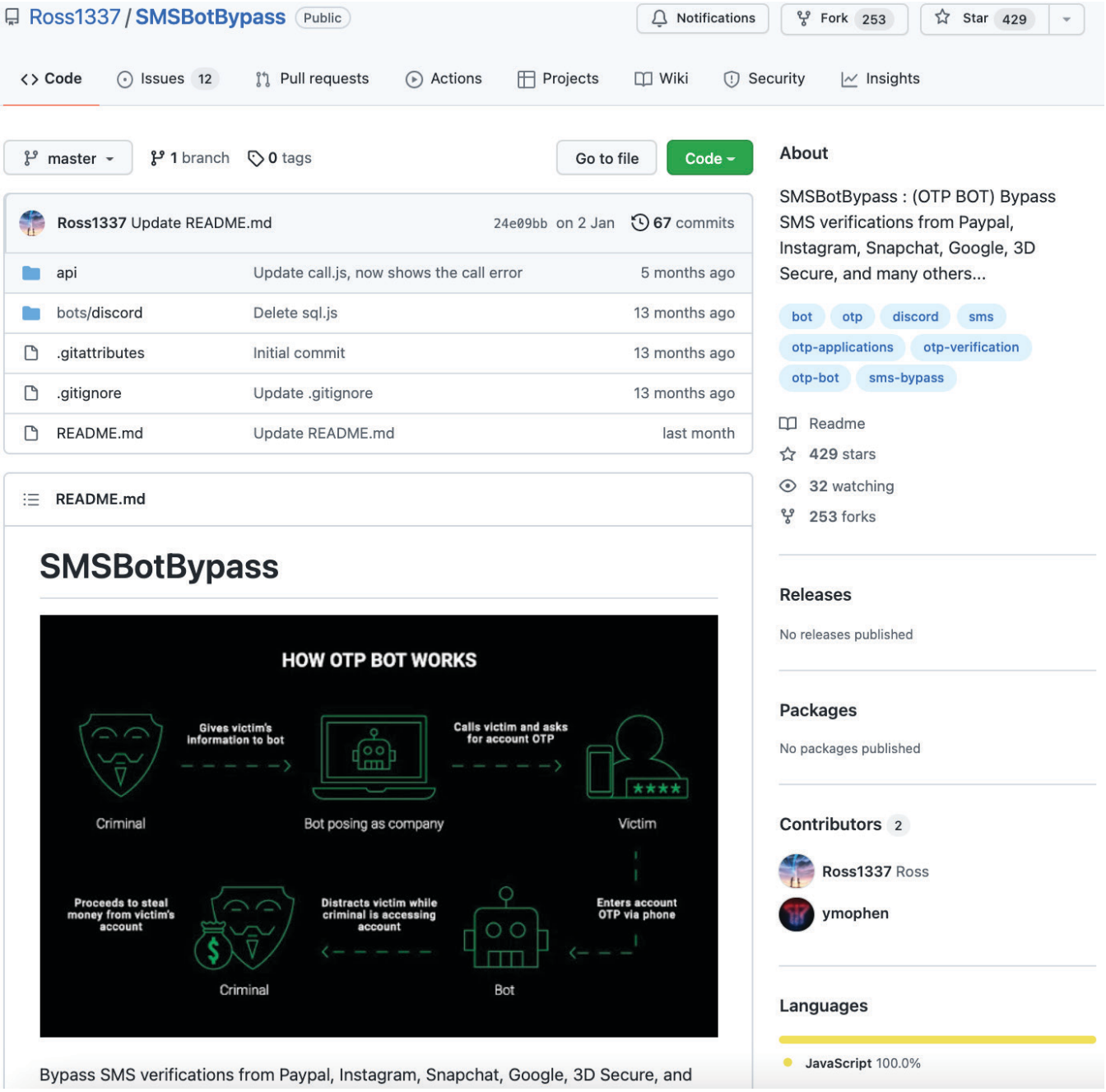


Figure 4: The main page of the SMSBotBypass page on GitHub (Source: GitHub)

Step-by-Step Tutorial for SMSBotBypass

SMSBotBypass is an open-source API that connects a threat actor's Twilio account with a Discord bot to provide a quick and simple-to-use method of initiating vishing calls and collecting inputted sensitive data. Recorded Future analysts tested SMSBotBypass and confirmed that it works as intended. Furthermore, configuring SMSBotBypass does not require a high level of technical expertise, and deploying the tool to target specific victims is very simple.

Pre-Deployment: Identifying Targets

A threat actor would only need to perform steps 1 and 2 once, when initially setting up the tool. From there, the threat actor would redo steps 3 and 4 according to different schemes or types of victims.

For bank fraud-focused schemes, threat actors would typically identify targets through "bank logs", records that include victims' login credentials for online bank accounts, cookies, and varying amounts of personally identifiable information. Threat actors could compromise bank logs themselves through phishing campaigns or malware, or purchase them on dark web marketplaces for a typical price of between $5 and $15.

For card fraud-focused schemes, the threat actor would only need to use a tool like SMSBypassBot if the given compromised payment card was 3DS-protected and monetized via a merchant using an OTP authentication flow. To determine whether a card is 3DS-protected, threat actors can use card checker services like CHK.CARDS and LuxChecker, which have recently begun launching 3DS card checks. If a card is 3DS-protected, the threat actor would need to obtain the cardholder's contact information to deploy SMSBypassBot. However, approximately 50% of card-not-present (CNP) records posted in the past year contain either the cardholder's email address or phone number. Therefore, in half of instances, the threat actor would already have this information on hand.

Step 1: Configuring the 3 Components: SMSBotBypass, Twilio, Discord

From December 26, 2020 to mid-February 2022, SMSBotBypass was freely available on GitHub and could be downloaded via the command "git clone https://github[.]com/Ross1337/SMSBotBypass.git". From there, users could install the API's dependencies.

Threat actors create a paid account on Twilio, a legitimate and highly popular service that offers web-based APIs for performing automated voice calls and sending text messages. In the next step, threat actors connect their Twilio account to SMSBotBypass via the Twilio API.

Threat actors create a Discord account to use a Discord bot. Discord is a social communication platform for messaging and calling that supports voice and video calls in addition to text-chatting. Users can communicate between themselves in private chats or as communities on servers. Users are able to add bots to servers to perform different tasks.

Step 2: Integrating Twilio and Discord Accounts into SMSBotBypass

First, a user must connect their Twilio account to SMSBotBypass by adding the Twilio AccountSid, AuthToken, caller ID, and an IP address (to run the web server) to the config.js file. When these fields have been added, SMSBotBypass should be operable once port 1337 (the port used by the API) has been opened. If the connected Twilio account is on a free trial, the user must open the test/call.js file and modify the phone number line (122) with a working phone number that the user can access. If the process does not work at this time, the Twilio account will need to be upgraded to a full account. A benefit for cybercriminals using Twilio for this purpose is the ability to set the speech language to any of the 26 supported dialects (18 languages and 14 locales), allowing a wider pool of victims.

The next step is setting up the Discord bot. The API password must be obtained from the API folder's config.js file, then input into the SMSBotBypass config.js file with the API URL, Discord bot token, and an IP address (to run the web server). Once these fields are input, the user needs to change the secret password for their personal use. The Discord bot should be ready to add to the Discord server, where a role will need to be created giving it permission to view and send messages. If it is set up correctly, the user is able to initialize the bot by sending the command "npm i" in a channel the bot can access.

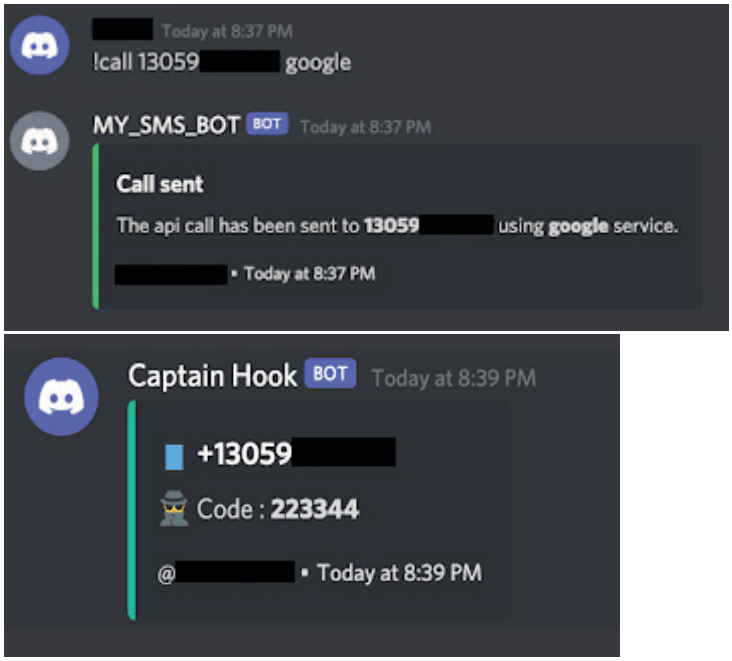
Step 3: Creating Customized Voice Calls for Specific Entities

Once a threat actor has configured SMSBotBypass, it is easy to create multiple, customized vishing scripts that are designed to target OTPs of specific entities (for example, a financial institution or an online service). To do this, the threat actors must draft a script mimicking an official call from the targeted service. When a satisfactory script has been drafted, the threat actor must create an audio file to be used in the calls, which they can do themselves or by using services available on the internet. Although the quality of these services is not very good, it has proved to be enough to deceive victims. Fraudsters can also use freelance services to hire voice actors to create the audio files for them as well.

Step 4: Targeting Victims and Collecting OTPs

Once the threat actor has compiled a library of customized voice-call scripts, they can use the Discord bot interface to quickly designate a target and initiate an automated call via Twilio. Should the target fall victim to the vishing attempt and input their OTP on their phone's keypad, the threat actor then receives the input OTP from the Discord bot interface.

Recorded Future analysts tested SMSBotBypass by going through each step of the process and simulating an attack against another Recorded Future analyst. The simulation was successful, indicating that the tool works as intended. In the simulation, analysts changed the default audio track to a custom track that simulated the Google Account Recovery Service. The analyst who acted as the victim received a call in which they were asked to enter an OTP delivered via SMS. The code that the analyst (the "victim") entered during the call was received by the other analyst (the "attacker") via the Discord bot. (Listen to an audio track of our simulated attack here.)



Figures 5 and 6: The code capture result from the simulated attack conducted by analysts (Source: Discord)

Mitigation

For individuals and financial institutions, the best methods of mitigating the risks of OTP bypass bots mirror well-established practices for mitigating phishing attacks more broadly.

If you receive a call, text message, or email from an entity claiming to be a representative of your financial institutions or a service that you use requesting any form of sensitive data, do not engage with the communication. Instead, navigate to the entity's main page and call the official customer service number to confirm if any action needs to be taken.

Financial institutions and service providers should develop a strategy and plan of action for communicating and informing clients about the risks of phishing. This plan of action should ensure that clients are aware of what types of information, if any, their representatives would request from a client.

Outlook

As long as OTPs remain a prominent form of MFA, threat actors will continue to seek out methods of bypassing them. While OTP bypass bots do not introduce a new technical method of bypassing OTPs, they do combine time-tested social engineering and vishing techniques with partial automation and easy-to-use interfaces. As a result, the main threats posed by OTP bypass bots is that they increase the scale of attacks that threat actors can conduct in a short period of time and deepen the pool of threat actors who are capable of conducting these attacks by dramatically reducing the technical and language barriers to entry. OTP bypass bots are typically affordable, require almost no prior experience to use, and do not require high-level language skills.

In terms of the specific OTP bypass bot detailed in this report, SMSBypassBot, Recorded Future analysts successfully conducted a simulated attack with the tool, indicating that it poses a threat to individuals and any institutions that use OTP. As of this report, GitHub has deleted this project and all forks from this repository; however, hackers have already downloaded the code from this project and are actively using it. Similar projects are likely to appear in the near future, leading to an increase in attacks of this type.

About Insikt Group®

Insikt Group is Recorded Future's threat research division, comprising analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence on a range of cyber and geopolitical threats that reduces risk for clients, enables tangible outcomes, and prevents business disruption. Coverage areas include research on state-sponsored threat groups; financially-motivated threat actors on the darknet and criminal underground; newly emerging malware and attacker infrastructure; strategic geopolitics; and influence operations.

About Recorded Future®

Recorded Future is the world's largest intelligence company. Recorded Future's cloud-based Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,400 businesses and government organizations across more than 60 countries.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.